BSA Principles for Good Governance: Supply Chain Risk Management

Managing security risks to information technology supply chains is an important priority for both governments and businesses globally. Information and communications technologies store, process, and transmit vast volumes of data, underpin the global digital economy and support the operations of governments, critical infrastructures, and societies. When malicious actors exploit supply chain vulnerabilities, they can cause unacceptable harm to privacy, security, and commerce. Yet, mistargeted policy interventions aimed at improving security can introduce unintended consequences by causing severe damage to the technologies and economic activities they seek to protect.

Effective government approaches to supply chain risk management recognize the global, interconnected nature of supply chains and the threats against them, identifying and disrupting malicious actors through policies and processes that are sustainable, reciprocal, and transparent.

As governments around the world seek to address supply chain risk management, BSA asserts the principles below to guide effective policy responses. BSA will use these principles to evaluate national supply chain risk management policies and to work toward enhancing the security, integrity, and vitality of the global digital economy.

Risk Management

Governments should adopt risk management approaches to supply chain security. Risk management entails understanding risk through the identification of likely threats, vulnerabilities and potential consequences, tailoring mitigation strategies to risks, and prioritizing actions based on the most relevant and potentially impactful risks. Risk management approaches retain flexibility that enable security practitioners within both governments and businesses to adapt to a constantly evolving threat environment. Finally, risk management approaches consider not only risks from malicious actors, but also the risks, timelines, and costs associated with potential mitigation options, helping policymakers avoid unintended consequences of mistargeted policies.

A corollary to this principle is that supply chain security policies should empower governments to take action based on security risks. Further, policies should foster, not hinder, global technology competition, and allow nations to meet their international trade commitments.

Interoperability

Modern technology supply chains are often transnational, and so too are threats against them. As such, effective policies will embrace interoperability – consistency and compatibility of regulations and technical standards across national borders – and will avoid adopting categorical prohibitions against the acquisition or integration of technologies simply because they are developed abroad. A good rule of thumb is: a government should adopt policies only to the extent it is comfortable with other governments enforcing those policies against its own businesses.

Building policies around internationally recognized, industry driven standards ensures that technology providers can develop, maintain, and secure innovative products across global boundaries and help to facilitate transnational operational collaboration against significant cyber threats.

Transparency

Opaque government supply chain risk management policies and processes, such as the debarment of certain foreign vendors from acquisition processes without notification or justification, create confusion and can prompt protectionist interventions by other governments, undermining the economic competitiveness of global businesses. Absent exceptional circumstances, government supply chain risk management policies and their implementation should be transparent to the public, with specific actions notified to impacted stakeholders. In any case in which a government denies market access to a vendor or technology, that government should articulate a public justification outlining specific security concerns prompting the action.

In addition, the transparency principle should oblige the government to provide for disclosure of identified supply chain vulnerabilities to suppliers, in accordance with vulnerability disclosure methodologies described in ISO/IEC 29147. Government vulnerability disclosure can improve the overall security of the digital ecosystem and improve public-private collaboration against supply chain threats.

Discretion

Enhancing supply chain security means, in part, developing a more secure global cybersecurity ecosystem that recognizes norms for responsible behavior and prioritizes collective defense against malicious threats. Governments should pledge that they will not undertake systemic interventions in global supply chains.

Enforcement

While state actors may present the most sophisticated threats, supply chains are also under constant pressure from non-state actors engaging in malicious cybersecurity activity, counterfeiting, product diversion, and related activities. A key element of a government's supply chain risk management strategy must be to pursue aggressive law enforcement against malicious actors within its jurisdiction.

Collaboration

Government supply chain risk management efforts will be most effective when undertaken in collaboration with key non-governmental stakeholders, including industry. As industry increasingly provides leadership on addressing supply chain concerns, governments should embrace creative opportunities for public-private partnerships aimed at securing supply chains and developing best practices for supply chain risk management. Recent efforts like the Paris Call for Trust and Security in Cyberspace are promising. Likewise, collaboration should be sought on a government-to-government basis with key partners through the expansion of supply chain threat information-sharing and operational cooperation against supply chain threats.

Fairness

Supply chain risk management processes should establish meaningful mechanisms for resolving disputes, including opportunities for impacted stakeholders to appeal or protest decisions, provide defense against any alleged offenses, and remediate past concerns. Dispute resolution mechanisms create an environment of certainty and predictability without limiting tools for mitigating risk.

Research and Development

Securing global supply chains will be an ongoing challenge – one in which security techniques must adapt to an ever-changing environment of new technologies and new threats. By investing in the research and development of new technological approaches to fostering supply chain integrity, governments can gain and maintain the advantage against malicious actors. Promising areas of research include the use of blockchain-based technologies, development of processes to vet third-party components for security issues, and the application of artificial intelligence for the analysis of supply chain data and anomaly detection, among others.